PURPOSE

This transmits IRM 1.16.2, Physical Security — Managers Security Handbook, which replaces IRM 1(16)12, Managers Security Handbook.

BACKGROUND

The IRM is being converted to a new format and style which will be issued in 8½ by 11" instead of the current 6" by 9" size. The new IRM 1.16.2 includes simplified text, a new numbering system, and a new format for organizing text.

The transmittal reissues existing information in the IRM format and provides new guidelines in management's responsibility for ensuring that established minimum security standards are being followed. It replaces text currently contained in IRM 1(16)12 which is obsolete.

NATURE OF MATERIALS

New IRM 1.16.2, Physical Security — Managers Security Handbook, provides guidance to managers on the minimum security standards.

INTENDED AUDIENCE

All Operating Divisions and functions.

Raymond E. Wiggins
for Thomas Liberti
National Director, Real Estate
Planning and Management Division

Table of Contents

Table of Contents

1.16.2.1 (03-12-2001)
Scope of the Managers Security Handbook

(1) The threats to security which the Service faces vary greatly with type, size and location of a particular facility or operation. It is impractical, therefore, to require rigid security procedures for “worst case” situations applicable to only a few locations or procedures that are designed to deal with problems which occur infrequently and have minimal impact when they do occur.

(2) This handbook includes the minimum security standards for the entire Federal Tax Administration System as administered within the Internal Revenue Service. Also included are requirements for the protection of tax returns, return information, cash, negotiable instruments and other sensitive information and documents. This handbook is designed to provide management with a basic framework of minimum security standards which gives greater flexibility and allows them to develop higher standards, when necessary, to meet the demands of the local situation.

(3) All managers are responsible for insuring that information is provided protection commensurate with its level of sensitivity and that all assets are protected against destruction, theft, or abuse. The minimum standards may provide adequate security for one functional area, while in another area management may determine a need to develop safeguards which exceed the minimum standards. These safeguards would not become the Service standard, but rather would be applied only to the functional area. This added flexibility requires continuing analysis of conditions in order to ensure the adequacy of security measures.

1.16.2.2 (03-12-2001)
Responsibilities of Real Estate and Facilities Management Division

(1) Only the Real Estate and Facilities Management Division has the authority to modify existing or create new minimum physical security standards. Requests for deviations will be submitted in writing through appropriate management channels to the Real Estate and Facilities Management Division, Attention: Safety and Security Branch.

(2) The Real Estate and Facilities Management Division is responsible for:

- reviewing and updating the minimum security standards, and other instructions in the security handbooks;
- conducting security program evaluations to ascertain compliance with the minimum security standards; and
- reviewing all National Office functional security procedures for Servicewide implementation for compliance with prescribed security standards and necessary coordination.

1.16.2.3 (03-12-2001)
Responsibilities of Service Officials, Managers and Employees

(1) Service officials and managers are responsible for ensuring the continued operation of the Federal Tax Administration System by taking all reasonable actions to prevent the loss of life and property, the disruption of services and functions, and the unauthorized disclosure of documents and information.

(2) Managers may find that in order to accommodate the unique needs of their organization, it is necessary to develop security measures that exceed the minimum standards. Head of offices are responsible for reviewing internal management documents that provide additional security measures for the unique needs of their organization. They must ensure that originators of security procedures for their function's Manual refer to the instructions in IRM 1.16.8, Physical Security Standards; that instructions of functional security procedures are routed through the Real Estate and Facilities Management Division for review and coordination before issuance; and that security measures taken are reasonable, adequate and effective.

(3) Exhibit 1.16.2-2 provides specific safeguards for the protection of particular items. The head of office must notify the Real Estate and Facilities Management Division of any changes to Exhibit 1.16.2-2 for which they are responsible.

(4) Managers must ensure that the physical security measures required for protecting information, property and life are applied within their area of supervision and that those measures meet the established minimum security standards. Above standard security requirements applicable to a manager's operation should be reflected in the security portion of their organization's part of the IRM.

(5) The emphasis on day-to-day responsibility for maintaining the security program has shifted from the Security function to managers. Every manager in the Internal Revenue Service is responsible for ensuring compliance with the minimum standards contained in this Handbook.

(6) Management at all levels will maintain effective controls to prevent fraud, waste, or abuse of Government resources and mismanagement of Service programs. The control systems will provide reasonable assurance that all resources are safeguarded from unauthorized use or disposition. The basic standards and tenets of the control system for all managers are:

- ***Documentation*** — Clearly written instructions for all financial transactions, accounting for resources and internal control requirements shall be readily available.
- ***Transactions*** — Transactions shall be recorded when executed and records shall be maintained to verify that transactions are made by authorized persons and are within the scope of their authority.
- ***Separation of Duties*** — Duties such as authorizing, recording, issuing and receiving, making payments and reviewing or auditing shall be assigned to separate individuals to minimize the possibility of fraud, waste or abuse going undetected.
- ***Supervision*** — Qualified and continuous supervision shall be provided to ensure compliance with procedures. Periodic reviews will be conducted by responsible managers.
- ***Access to Resources*** — Direct physical access to resources and indirect access by preparation or processing of documents shall be limited to authorized personnel

- ***Competent Personnel*** — Care shall be taken that key personnel are of high integrity and are competent by education, training, or experience to accomplish their duties.
- ***Reasonable Assurance*** — Internal control systems will provide reasonable assurance that the objectives of the systems should be met. The cost of controls should not exceed the benefits.
- ***Reporting Violations*** — All managers will ensure that possible violations of the internal control systems will be expeditiously reported according to established procedures.

(7) All employees must comply with established security procedures in protecting information, property, and documents with which they are entrusted.

1.16.2.4 (03-12-2001)
Limiting Access

(1) The guiding principle of security within IRS is ***"limiting access to assets based on need."*** This principle is the basic premise for most of our security programs. When applied to information security, this translates into limiting access to documents on a need-to-know basis. With regard to physical security, it means restricting entrance to rooms, areas or facilities based on the individual's duties or responsibilities.

(2) The need to maintain reasonable security at computing and processing centers at all times requires that only authorized visitors be permitted to enter the center. Providing tours for interested, non-tax related individuals or groups for purposes of orienting them with center operations is NOT authorized.

(3) Official visits by individual tax preparers, tax accountants, news media representatives and other professional tax oriented individuals and groups may be permitted at the discretion of the Director and in keeping with security requirements.

1.16.2.4.1 (03-12-2001)
Determining Need

(1) Determining the need to access information, documents, rooms, area or facilities is based on whether or not an individual needs access to perform assigned duties and responsibilities. ***Does the individual need to know? Does the individual need to enter a secured area?*** The determination of needs and the subsequent decision to grant access to an asset is a function of management. Once the determination is made, Security personnel should be consulted to assist in selecting the appropriate means to achieve the desired level of control.

(2) While the safeguards presented in this Handbook provide protection against environmental threats (fire, power failures, etc.) and acts of God (hurricanes, floods, etc.), most of the protection methods are designed to protect against such human threats as:

- unauthorized disclosure,
- unauthorized entry,
- vandalism,
- fraud,

- theft,
- accidental/deliberate alteration or destruction of information or property,
- sabotage,
- demonstrations/riots.

(3) Most of the methods of protection are designed for protection after normal duty hours or at any time the assets to be protected are not under personal custody of authorized Service employees. The methods of protection are also designed to limit access by non-IRS, non-Federal individuals who may require access to Service facilities.

(4) Because any single safeguard is often insufficient protection for any asset, the concept of layering of safeguards was developed to provide security in depth. To facilitate understanding security in depth, it is important to have some understanding of what must be considered before a decision can be reached regarding the appropriate safeguard, or combination of safeguards, required for a particular asset. The value of the asset and any applicable laws are the primary considerations. Once these are determined, then the problem of unauthorized access is approached by one or all of these methods:

- deter
- delay
- detect
- respond
- deny

Exhibit 1.16.8.1-1 in IRM 1.16.8, Physical Security Standards, provides additional information on safeguards and their related protection functions.

1.16.2.5 (03-12-2001)
Protection of Information, Facility, Property and Personnel

(1) The physical security program should protect information, facilities, property and personnel while preserving the environment in which the Service's mission may be carried out without disruption. It should do this without being so restrictive that security itself becomes a disruption.

(2) Ideally, physical security measures should provide a facility with absolute protection from a host of threats. However, due to physical, operational, and financial limitations, absolute security is neither possible nor practicable. Therefore, a practical approach to physical security is essential and will protect information, facilities, property and personnel by employing a combination of measures to deny, deter, detect and/or apprehend unauthorized entrants without being so restrictive that security itself becomes a disruption.

1.16.2.5.1 (03-12-2001)
Minimum Protection Standards (MPS)

(1) The Minimum Protection Standards (MPS) system establishes a uniform method for protecting data and items which require safeguarding. This system contains minimum standards which will be applied on a nationwide basis. The MPS system has been designed to provide management with a basic framework of minimum security requirements which will provide greater flexibility in dealing with local conditions. Since

local factors may require additional security measures, management must analyze local circumstances to determine space, container and other security needs at individual facilities. (See IRM 1.16.8, Physical Security Handbook.)

(2) **Standard** — Items and data to be protected are divided into three groups:

a. Normal Security (NS) — All information which has not been identified as requiring High Security or special protection,
b. High Security (HS) — Items which require greater than normal security due to their sensitivity and/or the potential impact of their loss or disclosure,
c. Special Security (SP) — Items which require a specific type of containerization, regardless of the area security provided, due to special access control needs.
d. All protectable items must be afforded a minimum of locked container, perimeter, interior or secured area of protection. (Exhibit 1.16.2-1 identifies protective requirements and Exhibit 1.16.2-2 provides a list of protectable items and their security designations.)

(3) Containers — Containers are grouped into three categories:

a. Lockable container — any metal container with riveted or welded seams which is locked and to which keys and combinations are controlled,
b. Security container — lockable metal container that has a tested resistance to penetration and is approved for storage of high security items (e.g. metal lateral key lock file w/security modifications, metal lateral file equipped w/lock bars on both sides, etc.),
c. Safes and vaults — Safes which have been accepted for general use by the Service can be identified by GSA approval as Class I, II, IV or V or Underwriters Laboratories Listings of TL-30, TRTL-30, TRTL-60 or TXTL-60. Vaults must have been constructed to specifications approved jointly by IRS and GSA.

(4) All space can be classified as either secured or non-secured. Secured areas are perimeter and/or internal areas which have been designed to prevent undetected entry by unauthorized persons during non-duty hours.

1.16.2.5.2 (03-12-2001)

Space Planning

(1) It is imperative that security considerations be addressed whenever IRS space is designed, acquired, altered or redesigned. Failure to consider adequate security during the early phases of space planning generally will result in costly modifications. In “open space” environments, the Service must ensure that acoustical planning is considered in order to minimize the potential for inadvertent unauthorized disclosures and to achieve an acceptable level of ambient noise. In addition, with the increased use of automated systems, it is important to consider placement of computer terminals in “open space” in order to avoid unauthorized disclosures.

(2) **Standard** — Managers within the space and security functions are mutually responsible for:

1. Developing local procedures which reflect shared responsibility, necessary coordination and mutual approval in order to assure that both organizations are timely notified of plans for design or redesign of new or existing space,
2. Coordinating requests for procurement of guard services, security devices, waste destruction, and other services (keys, locks, containers), and
3. Utilizing sensor/detection devices or making sure protectable items are stored in locked containers during non-duty hours if restricted areas are co-located within non-restricted areas.

(3) All managers will ensure that space planning, particularly in “open space” environments, provides:

a. perimeter security commensurate with the needs of the most critical operations to be performed in the office;
b. use of barriers, as needed, to separate operational areas and minimize traffic;
c. aural and visual privacy to minimize inadvertent disclosures of tax and privacy data, and
d. appropriate containers for the storage of protectable items during non-duty hours.

1.16.2.5.3 (03-12-2001)

Restricted Areas

(1) Under the Restricted Area concept, entry to critical areas is controlled and access is limited to those individuals who actually work in the area or have demonstrated a bonafide need to enter the area. Thus, the term restricted area denotes an area to which entry is restricted to authorized personnel only during normal working hours. The use of restricted areas is an effective method of controlling the movement of individuals and eliminating unauthorized traffic through critical areas, thereby reducing the opportunity for unauthorized disclosure, theft or alteration of tax information. All restricted areas will also be secured areas as defined in Chapter 5 of IRM 1.16.8, Physical Security Standards, or provisions must be made to store protectable items in appropriate containers during non-duty hours.

(2) **Standard** — All managers will work with the local security office to determine the best method of complying with restricted area security requirements. All managers will assure that:

a. Restricted areas are prominently posted and separated (ropes and stanchions are not acceptable) from non-restricted areas by physical barriers which will control access.
b. The number of entrances are kept to a minimum, and each entrance will be controlled. At entrances equipped with card readers, employees assigned to the area will use his/her access card and pin number (if required) to unlock the door every time he/she enters the

area. At entrances not equipped with card readers, a monitor will control access by having authorized employees display their ID card each time they enter the area.

c. Appropriately coded ID cards are worn at all times by all personnel within each restricted area. Any individual in the area not wearing an appropriately coded ID shall be immediately reported to the supervisor.

d. At a minimum, a trained monitor will be located at the main entrance of each restricted area. The monitor is responsible for assuring that only authorized personnel with an official need enter the area. If any unauthorized individual attempts to access the area, the monitor should immediately report the attempt to the manager.

e. A Restricted Area Register (Form 5421) will be maintained at the main entrance of each restricted area and all visitors will be directed to this entrance to sign the register, show appropriate identification and be assigned a visitor ID. The Register will be closed out at the end of each month, reviewed by the restricted area supervisor and forwarded to the branch chief. The branch chief will review the register and retain it in the branch office for at least one year.

f. An Authorized Access List will be prepared monthly and will be maintained at the main entrance. This list will have names of employees who have a frequent and continuing access need. The Branch Chief must validate the need prior to dating and signing the list.

1.16.2.5.4 (03-12-2001)
Secured Areas/Perimeters

(1) The standards previously presented for restricted areas dealt with the need to control access to selected areas during normal work hours. Secured area/perimeters are used to control access during non-work hours. Since no employees are present during non-work hours to prevent unauthorized persons from entering the area, various safeguards are used to secure the protectable materials.

(2) **Standard** — Secured areas are perimeter and or internal areas which have been designed to prevent undetected entry by unauthorized persons during non-duty hours. All managers whose operations are located in restricted and secured areas will ensure that the safeguards used to protect the secured area are functioning and that all employees are familiar with these operations. The local Security office will assist in determining the best method of compliance with the secured area/perimeter security.

1.16.2.5.5 (03-12-2001)
Controlled Areas

(1) In some offices, managers may have a need to control access between work areas during duty hours for production or other administrative reasons. The functions performed in the area do not require the constrictive measures required for restricted areas but do require minimal control over access.

(2) **Standard** — Local management may determine that areas under their jurisdiction require some form of access control. Controlled areas can be

established as local management determines. The need for access control for these areas should be thoroughly documented for subsequent review. If local management wishes to use one or more of the formal security controls, such as ID card identifiers, security registers, etc. concurrence from the Security office is necessary. It is not permissible to use all of the formal restricted area security controls for a controlled area.

1.16.2.5.6 (03-12-2001)
Key and Combination Control

(1) Keys, key cards and combinations to locks are a means of controlling access. Access to a locked area or container can be controlled only if the key, key card or combination is controlled. The security provided by a particular locking system is lost if the key, key card or combination is not strictly controlled or becomes compromised in any way.

(2) **Standard** — Managers must ensure that keys, key cards and combinations are issued only to persons with an official need to access the area or container and that these persons are reminded of their responsibility to safeguard these items. Individuals assigned keys, key cards and combinations may not share these with any other individual unless approved by the manager and only if there is an official need.

a. Combinations must be memorized and not written on note pads, calendars, etc. Requests for door keys (including card keys) and door key duplications will be approved by the Security function. Groups of keys to a particular area may be issued to the responsible manager for their control and issuance. No more than three (3) keys are authorized for each security container.
b. All keys will be issued and accounted for on a Form 1930, Custody Receipt for Government Property or comparable form. Accountability records (Forms 1930) for container keys will be maintained by area management and must include an inventory of total keys available for each container. Combinations will be recorded on a Form 700, Security Container Information, which will be maintained at the next higher level of management with the procedure terminating in the Security function or Facilities function and will be stored in a container which provides at least the same degree of protection.
c. Combinations must be changed whenever an employee who knows the combination leaves on a job transfer, retires, or terminates employment; whenever the combination is compromised in any way; at least once a year; or when the safe or lock is originally received. Combinations should be at least four (4) digits.
d. Criminal Investigation will maintain their own key and combination control, complying with the above standards, except no approval for duplicate keys is required by the Security function and control of Forms 1930 and 700 will remain in Criminal Investigation only.

1.16.2.5.7 (03-12-2001)
Information Security

(1) The protection of information is of vital concern to the Service. All employees of the Service that have or have had access to tax returns or return information and privacy information are prohibited by statute from disclosing such information except as authorized by applicable law or

regulation (see IRM 1.3, Disclosure of Official Information Handbook). In addition to tax data there are many other documents that require protection from disclosure.

(2) **Standard** — Every effort must be made to ensure that all documents are provided protection commensurate with the information therein. Tax data and privacy information shall be properly protected during duty and non-duty hours, transmitted in a traceable manner, and protected from inadvertent disclosure when in use. Documents containing information that require protection must be stored in accordance with minimum protection standards whenever they are not in the custody of an authorized IRS employee (see Exhibit 1.16.2-2).

1.16.2.5.8 (03-12-2001)
Privacy Act Information

(1) The Privacy Act of 1974, 5 U.S.C. 552a, provides comprehensive statutory recognition of an individual's right to privacy. Recorded information which is retrieved by reference to a name or other personal identifier, such as a social security number, is privacy information. The purpose of the Act is to give citizens more control over what information is collected about them by Federal agencies and how that information is used. The Act specifies that agencies will establish appropriate administrative, technical, and physical safeguards to insure the security of records and protect records against any anticipated threats or hazards to their security or integrity which could cause substantial harm, embarrassment, inconvenience, or unfairness to any individual about whom information is maintained (see IRM 1.3, Disclosure of Official Information Handbook).

(2) **Standard** — Managers will ensure Privacy information is protected from inadvertent disclosure when in use, stored in a manner that will prevent unauthorized access during non-duty hours, and destroyed by an approved method (i.e. shredding, pulping, disintegration or burning).

1.16.2.5.9 (03-12-2001)
Informant Information

(1) Persons furnishing information on tax violations expect and deserve to have their identity kept secret. All employees must, therefore, handle such information in strict confidence. Such information must be given special handling to avoid disclosure to other than those employees having a need to know.

(2) **Standard** — As soon as informant correspondence is recognized by mail classifiers or other employees, it will be sealed in a "To Be Opened By Addressee Only" envelope (E-19 or E-20) and routed to the Criminal Investigation office. These same precautions will also apply to claims for rewards, memorandums of interviews with informants, or any other communication which might in any way identify informants. The routing of informant communications to other activities by the Criminal Investigation activity will be made by transmission in sealed envelopes bearing instructions "To Be Opened By Addressee Only" or by hand carrying the material to the appropriate office. In order to maintain maximum security, informant communications, claims for rewards, reward reports,

memorandums or other documents which identify informants will be afforded containerized protection at all times, except when such documents are being processed. Access to such storage containers will be limited to the person/persons responsible for the security of the documents.

1.16.2.5.10 (03-12-2001)

National Security Information

(1) "National" security information is any information, regardless of form, pertaining to the national defense or foreign relations of the United States, that is owned by, produced by/for, or is under the control of the U.S. Government. Executive Order 12958 prescribes a uniform system for classifying, safeguarding, and declassifying national security information. "Classified national security information," commonly referred to as classified information, is information that requires protection against unauthorized disclosure. Classified information is marked **Top Secret, Secret,** or **Confidential** to indicate its classified status when in documentary form. Executive Order 12968 established the Federal personnel security program and addresses national policy for access to classified information. Access to classified information is guided by two principles: eligibility or "need for access" and "Need-to-know". Eligibility is a determination, commonly referred to as a "security clearance" (Top Secret, Secret or Confidential), that an employee requires access to a particular level of classified information to perform a lawful and authorized government function. "need-to-know" is a determination by an authorized holder of classified information that the prospective recipient requires access to a particular level of classified information in order to perform or assist in a lawful and authorized governmental function.

(2) **Standard** — Classified information shall be classified, declassified, safeguarded and controlled in a manner that prevents its unauthorized disclosure. An unauthorized disclosure is a communication or physical transfer of classified information to an unauthorized recipient. Employees shall not be granted access to classified information unless they have a security clearance at the appropriate level (Top Secret, Secret, Confidential); have a demonstrated need-to-know; and have signed an approved nondisclosure agreement. See IRM 1.9, National Security Information Handbook, and Chapter 11, of IRM 10.3.1, Internal Security Handbook.

1.16.2.5.11 (03-12-2001)

Officially Limited Information

(1) Sensitive But Unclassified (SBU) information is any information the loss, misuse, or unauthorized access to or modification of which could adversely affect the national interest or the conduct of federal programs, or the privacy to which individuals are entitled to under section 552a of Title 5 (the Privacy Act) or other laws. SBU is also known as *official limited information*. U.S. Government SBU may be marked with protective legends such as ***Limited Official Use, Official Use Only, For Official Use Only, Close Hold, Eyes Only, Law Enforcement Sensitive, Proprietary, and Restricted.*** SBU may be unmarked information such as medical, personnel, financial, investigative, law enforcement, regulatory, compliance, taxpayer data, security plans, and

procedures or countermeasures. Limited Official Use (LOU) is a category of SBU authorized within the Department of the Treasury. Official Use Only (OUO) information is a category of SBU information authorized within the Internal Revenue Service. Unauthorized disclosure of SBU may reduce the effectiveness of the Tax Administration system, violate law, or adversely affect the national interest, conduct of Federal programs, or the privacy to which individuals are entitled under the Privacy Act. SBU can be in paper, electronic, or material form. Regardless of its form or markings SBU information requires special handling to prevent its loss, misuse, alteration, or unauthorized disclosure.

(2) **Standard** — Managers at all levels are responsible for security of information under their control regardless of its form and for ensuring the information is properly safeguarded. (See IRM 1.16.5, Sensitive But Unclassified Information, Delegation Order 89, IRM 1.3, Disclosure of Information Handbook, and IRM 2.1 Information Systems.)

1.16.2.5.12 (03-12-2001)
Records and Documents

(1) All records and documents created or received by the Service in connection with operational and administrative activities are official information and the property of the United States Government. In accordance with 18 U.S.C. 2071, it is unlawful to remove records or documents from the custody of the Service except in accordance with prescribed procedures. The Tax Reform Act of 1976 provides that returns and return information are to be confidential and not subject to disclosure, except as specifically provided in IRC 6103 or other sections of the Internal Revenue Code. IRM 1.3, Disclosure of Official Information Handbook, contains guidelines governing the release of data included on tax returns and other information contained in Service files.

(2) **Standard** — Records and documents in the custody of Service employees will not be disclosed to the public, except through approved disclosure procedures, and will be protected from disclosure to other employees that do not have a need to know the information. In addition to guarding against unauthorized disclosure of tax information by Service employees, steps must be taken to prevent the possibility of such disclosures by non-Service personnel. Care must be taken to deny unauthorized non-Service personnel access to areas other than those which have been established for serving the public. All those persons with “a need to know,” such as certain Government contractors and vendor personnel, must be informed of the protection requirements under the law to prevent unauthorized disclosure. This can be best accomplished in writing, citing the prohibitions, restrictions and penalties for unauthorized disclosure of tax return and return information.

1.16.2.5.13 (03-12-2001)
Mail

(1) A large volume of the Service’s assets such as tax returns, remittances and government checks are transmitted by mail. The theft of mail can easily occur when left unattended on receiving docks or in building lobbies without protection.

(2) **Standard** — Incoming mail, not being distributed or processed, will be stored in a secured area or in locked containers. Mail, incoming or outgoing, will not be left unattended in areas open to the public.

1.16.2.5.14 (03-12-2001)
Protection at Taxpayer's Site

(1) At times field employees have sensitive information at the taxpayer's site which should be stored at an IRS facility. Due to local conditions, it is not always possible to remove the information from the taxpayer's site and store it at an IRS facility. Service managers must ensure that employees adequately secure such information at the taxpayer's site.

(2) **Standard** — IRS employees are responsible for securing sensitive tax information while at the taxpayer's site. Sensitive tax information, such as agent's work papers, original returns, examination plans, fraud data, etc., which is housed at a taxpayer's site must be stored in a security container under the control of the responsible Service employee. The taxpayer cannot have access to this container. If a security container is not available, this data may not be stored on the taxpayer's premises during non-duty hours. During duty hours, the data must be under the personal custody of the Service employee when it is not containerized. Personal custody exists when a responsible Service employee or other designated person (e.g. armored car service employee, authorized employee of a contract firm) has possession of, or visual contact with, a document or item of property. For the purpose of this definition, visual contact is limited to the person's desk or immediate work area over which he/she has physical control.

1.16.2.5.15 (03-12-2001)
Protection Outside of IRS Offices

(1) While on official travel it is often necessary for employees to carry tax data, laptops, taxpayer's checks and money orders, etc. Employees are held responsible for the loss, theft or disappearance of Service property when attributable to negligence. Recovery of documents may not necessarily be a mitigating circumstance after the loss.

(2) **Standard** — All sensitive information must be provided adequate safeguards. Employees in custody of sensitive information or Service property while outside of an IRS office must protect such items to the maximum extent possible. Managers shall caution employees against leaving information or Service property in automobiles, motel/hotel rooms, public conveyances, taxpayer's offices, etc. If there is no alternative and tax information must be left in a vehicle, it must be locked in the trunk. However, the vehicle must be locked and the material unattended for only a short period of time. It may not be stored in a vehicle overnight.

1.16.2.5.16 (03-12-2001)
Transmission

(1) The Service routinely ships tax returns and return information between IRS locations, as well as to other Federal and state agencies. Such data in transit is especially vulnerable to loss, destruction and disclosure. Such loss could result in irreparable damage to the Service or taxpayers, delay tax processing, and damage the public image of the IRS. (See IRM 1.16.8, Physical Security Handbook, Chapter 3.)

(2) **Standard** — All shipments of tax returns and return information from any processing or computing center, regional or district office, posts of duty, or other agencies and jurisdictions will be documented and monitored to ensure accountability and receipt for each shipment. Every Service facility engaged in the shipment of tax returns and tax information shall designate individuals to be responsible for monitoring the shipments.

1.16.2.5.17 (03-12-2001)
Disposition and Destruction

(1) The purpose of destroying waste material generated in the processing of tax documents or other related documents is to prevent the information from being disclosed to unauthorized personnel. Disposition and destruction of tax information must be in accordance with IRM 1.15.2 (Records Disposition Handbook).

(2) **Standard** — Although IRS employees may know the proper methods of destroying tax data, management must reinforce this knowledge by including document destruction as a topic in orientation sessions, periodic group meetings and other awareness sessions. Managers will ensure that waste material generated in the processing of tax documents, protected data or other related documents must be destroyed by shredding, pulping, disintegrating or burning or any other manner which in the judgement of the responsible security official renders the information contained in such material irrecoverable.

1.16.2.5.18 (03-12-2001)
Clean Desk Policy

(1) After-hours security reviews have identified repeated security violations where tax and privacy data are left out in work areas. To improve the level of protection provided tax and privacy data, the Service has adopted a clean desk policy. This initiative particularly lends itself to non-secure areas.

(2) **Standard** — All tax and privacy data when not in the custody of an authorized IRS employee must be stored in locked containers. Protected data must be locked in containers in areas where non-Service personnel may have access during non-duty hours. Security personnel will assist managers in determining when locked containers will be required. Directors, Submission Processing/Computing Centers, Customer Service Sites and other executive levels may exempt certain mass processing areas (pipeline type operations), but the exemption must be justified (e.g. containerizing will be so disruptive as to cause critical delays in processing) and documented and not just a matter of convenience. Items identified as requiring Special Security (SP) may not be exempted from the clean desk policy. Due to special access control needs these require a specific type containerization regardless of the area security provided. (For additional information see IRM 1.16.8, Chapter 4, section 4.2.)

1.16.2.5.19 (03-12-2001)
Security Awareness

(1) A security program is enhanced when all managers and all employees are aware of security requirements, including the reasons for each of the security requirements they are expected to follow or enforce. Security awareness is encouraged and strengthened by the attitudes and actions

of managers. If managers can explain the need for security in various situations, the employees will usually accept the need as an integral part of their responsibilities. The key to an awareness program is to show how the requirements relate to the work in which an employee is involved. For example, awareness efforts directed toward computer room employees should relate to security requirements in a computer room, while those efforts directed toward a tax auditor should relate to protecting the privacy of the taxpayer and the sensitivity to the tax return and return information.

(2) **Standard** — To ensure that all employees and managers are made aware of security requirements, a security awareness program will be implemented. Every security awareness program will include the following:

a. An annual security briefing, by security personnel, given to all managerial personnel on their responsibilities. The information presented will be passed on to employees by managers afterwards.
b. Security as a regular topic at periodic managerial meetings.
c. A security orientation of all new employees within the first week following employment. All seasonal employees will be given a refresher orientation during their first week or if they have been in non-work status for at least nine months. Local management will determine who will provide the orientation.
d. Periodic security briefing sessions conducted throughout the year by all processing/computing center supervisors will be provided. Security briefing sessions will also be provided at the beginning of each filing season.
e. A briefing of each employee of special security requirements pertaining to their particular work area will be provided by managers. The briefing will occur within the first 30 days of the date the employee reports for duty.

1.16.2.5.20 (03-12-2001)

Protection During Office Moves

(1) When it is necessary for an office to move to another location, plans must be made to properly protect and account for all tax data and other information, as well as government property. The circumstances of the move must be carefully considered (e.g., the distance involved and the method to be used in making the move).

(2) **Standard** — Managers will make sure that tax documents and other sensitive information is kept in locked cabinets or sealed in packing cartons while in transit. Accountability will be maintained to ensure that cabinets or cartons do not become misplaced or lost during the move. This can be accomplished by numbering the cabinets or cartons and maintaining a corresponding list of the numbered cabinets/cartons and what each contains. Throughout the move, classified material and other critical material will remain in the custody of an IRS employee with the appropriate clearance and need to know. The precautions taken to protect Government property during the move will be commensurate with the type and value of property involved. Small items of high value will be packed in cartons or moved in locked cabinets. Accountability will be maintained throughout the move.

1.16.2.6 (03-12-2001)
Emergency Planning

(1) The Tax Administration System is of vital importance to the economy of the United States and its protection must be assured at all times. To provide adequate protection, it is necessary to develop plans and procedures that will reduce the affect of incidents and emergencies. Incidents and emergencies are any situation or condition in or around an IRS facility that could deny access, cause damage to the facility or harm to employees. (See IRM 1.16.6, Emergency Management Handbook.)

1.16.2.6.1 (03-12-2001)
Reporting Incidents

(1) One aspect of emergency management is the timely reporting of significant conditions or situations. Prompt reporting of incidents is essential in order to advise all levels of management of conditions that affect the operation of the Service. Trends or patterns detected as a result of the analysis will assist in development of effective countermeasures to minimize the effect of future disruptions. Significant incidents must be reported to executive levels so that they may be aware of situations that could require their immediate assistance or that result in the need to respond to inquiries from Treasury, other Federal agencies or the news media. (See IRM 1.16.6, Emergency Management Handbook, Chapter 1.)

(2) **Standard** — Managers are responsible for making sure that significant incidents, unusual situations, potential incidents or situations affecting or which may affect the operations of the Service are reported as quickly as possible. Managers must make sure that all employees are familiar with incident reporting procedures and have access to the names and numbers of authorities charged with responding to incidents.

1.16.2.6.2 (03-12-2001)
Occupant Emergency Plans

(1) Occupant emergency plans are an essential part of a security program. Properly developed plans can reduce the threat to personnel, property, and other assets while minimizing work disruption. (See IRM 1.16.6, Emergency Management Handbook, Chapter 2.)

(2) **Standard** — The General Services Administration requires that occupant emergency plans be prepared for all federally occupied space. If the Service is the primary occupant agency, that is the agency with the largest population in the facility, the designated official will develop, maintain and test the occupant emergency plan. (The designated official is the highest ranking official of the primary occupant agency.) All possible situations should be addressed so that personnel will know what procedures to follow. Situations and incidents which should be included are: bomb threats, explosions, demonstrations, utility disruptions or failures, natural disasters, disruptive weather, fires, accidents, etc. Managers are responsible for ensuring that employees are familiar with the plan and with evacuation procedures.

1.16.2.6.3 (03-12-2001)
Business Resumption

(1) A Business Resumption Plan is a guide to the orderly re-establishment of operations after an incident. The objective of the plan is to resume

processing of critical functions as quickly as possible and eventually resumption of full, normal operations. (See IRM 1.16.6, Emergency Management Handbook, Chapter 3.)

(2) **Standard** — A properly developed plan requires coordination with all IRS organizations located at the facility. Each function will participate in the development of the plan by identifying critical needs (i.e. critical personnel and equipment needs, etc.) and will assign personnel to participate in the planning process. Emergency management planning must include not only recovery of critical information systems and applications but must also address issues such as human resources, vital records, telecommunications, security, environmental concerns and the facility which houses the work environment.

1.16.2.7 (03-12-2001)

Identification Media

(1) Internal Revenue Service identification media are issued solely for use by authorized employees in the performance of official duties. Authorized forms of Service identification are:

- ID card — issued to all employees for visual identification;
- Non-Enforcement pocket commissions — designed to show proof of authority and issued only to authorized employees;
- Enforcement pocket commissions — designed to show proof of authority and issued only to Criminal Investigation personnel in the 1811 series;
- Enforcement Shield — designed to provide an outward, visible sign of authority and issued only to Criminal Investigation personnel in the 1811 series; and
- Calling cards — designed to provide a ready reference for contact with non-Service individuals.

(2) Standard — Managers will ensure that Internal Revenue Service employees possess and display only authorized identification media and that such media be used and displayed properly. Identification media not officially authorized by the National Office Real Estate and Facilities Management Division may not be produced, procured or displayed. Section 499, Title 18 of the U.S. Code, prescribes a penalty of $2,000 or five years imprisonment or both for “Whoever falsely makes, forges, counterfeits, alters, or tampers with any naval, military, or official pass or permit issued by or under the authority of the United States, or with intent to defraud uses or possesses any such pass or permit, or personates or falsely represents himself to be or not to be a person to whom such permit has been duly issued or willfully allows any other person to have or use any such pass or permit issued for his use alone.” Section 701, Title 18 of the U.S. Code prescribes a penalty of $250 or six months imprisonment or both, for “Whoever manufactures, sells or possesses any badge, identification card or other insignia of the design prescribed by the head of any department or agency of the United States for use by any officer or employee thereof, or any colorable imitation thereof, or photographs, prints, or in any other manner makes or executes any engraving, photograph, print or impression in the likeness of any such badge, identification card, or other insignia, or any colorable imitation

thereof, except as authorized under the regulations made pursuant to law." (See IRM 1.16.4, Identification Media Handbook, Chapter 1.)

1.16.2.7.1 (03-12-2001)
Identification Card

(1) ID cards will be issued to all Service employees and will be worn while in Service facilities. In order to preserve the integrity and reliability of the ID card, employees may never have more then one ID card in their possession and all ID cards must be recovered from personnel who leave the Service. (See IRM 1.16.4, Identification Media Handbook, Chapter 2.)

(2) **Standard** — All managers and supervisors have responsibility for:

- ensuring that employees under their supervision are issued ID cards and wear them properly at all times,
- recovering, properly securing and sending to the Security function all ID cards from their employees who leave the Service or who are no longer authorized to have ID media,
- reporting any lost or stolen ID cards to the local Security function (if restricted area ID or if the employee is on an access list, also notify the restricted area manager),
- reminding employees of their responsibility to safeguard their ID card,
- reminding employees who leave the Service of their obligation to turn in their ID card on the last workday,
- requesting replacement of ID cards for their employees, as necessary, and
- ensuring that employees under their supervision follow all Service and local procedures when in Service facilities.

1.16.2.7.2 (03-12-2001)
Access by Other Federal and Non-Federal Personnel

(1) Because of the need for other Federal personnel and non-Federal personnel (e.g. GSA, contractors, vendors) to have access to Service facilities, procedures have been established to meet this need while still providing appropriate safeguards. While these individuals may have a need to be in an IRS work area, they are not IRS employees and are not provided the same privileges and access levels. When visitors are in the work area, care must be taken to prevent unauthorized disclosures.

(2) **Standard** — Managers are responsible for ensuring that other Federal personnel and non-Federal personnel follow all Service and local procedures while in IRS facilities. Managers are responsible for advising employees when visitors are in the work area and reminding them that sensitive information is not to be discussed or left in view of visitors.

1.16.2.7.3 (03-12-2001)
Issuance of ID Cards to Non-Federal Personnel

(1) With the growing use of outside expertise, the demand for staff-like access (unescorted access in IRS facilities or work areas) by non-Federal personnel to IRS facilities has greatly increased. In order to meet this demand, non-Federal personnel who have a daily need on a continuing basis to access a facility over a period of time (usually more than two weeks) may be issued a red-photo ID card.

(2) **Standard** — Managers, in organizations utilizing non-Federal personnel, are responsible for ensuring that these individuals are properly badged and are aware of and follow all Service and local procedures. The Security function must be notified in writing of the impending visit, length of the visit, names of the individuals and whether background checks have been conducted, where appropriate. Non-federal ID cards (Forms 6056) may not be removed from the issuing facility and may not be used as authorization to access Service facilities.

1.16.2.7.4 (03-12-2001)
Issuance of Visitor ID Cards

(1) Other Federal personnel and non-Federal personnel may have a need to visit IRS facilities. These individuals do not require staff-like access but may need periodic access on a regular basis. These individuals may be issued a non-photo, "VISITOR" ID card.

(2) **Standard** — Managers are responsible for ensuring that individuals visiting an IRS facility are placed on a visitors register and upon arrival are made aware of and follow all Service and local procedures. These individuals may not be given staff-like access but rather should, in most instances, be limited to a specific work area and be escorted to that work area by an IRS employee or at a minimum an IRS employee must certify need to access. Visitors must be on a visitors register, show a picture ID to verify identity and sign the visitor's register. Employees are to be notified that there is a visitor in the work area and that sensitive information is not to be discussed or left in view of visitors. The "VISITOR" ID card may not be removed from the facility but must be recovered upon exiting.

1.16.2.7.5 (03-12-2001)
Escort Only ID Cards

(1) Non-federal personnel, visiting an IRS facility, who do not have a verified background check or who are not on a visitor list, must be issued an "Escort Only" ID card. This is a non-photo ID card that will be issued only after the individual shows a picture ID, signs the visitor register and is verified by an IRS employee assigned to the facility. The visitor will be escorted at all times by an IRS employee.

(2) **Standard** — Managers are responsible for ensuring that individuals issued "Escort Only" ID cards are escorted at all times by an IRS employee and that these individuals follow all Service and local procedures. Managers will ensure that the visitor's need to access has been validated by an IRS employee assigned to the facility. Managers are responsible for notifying employees that there is a visitor in the work area and that sensitive information is not to be discussed or left in view of the visitor.

1.16.2.7.6 (03-12-2001)
Pocket Commissions

(1) Pocket commissions are used to present proof of authority in the performance of official duties. They are primarily intended to identify Service personnel to the public when dealing with tax matters and may not be issued merely to identify employees for transaction of routine business. There are two categories of pocket commissions—enforcement

and non-enforcement. Enforcement commissions are issued only to individuals in the 1811 series. Non-enforcement commissions are issued to all other authorized employees. (See IRM 1.16.4, Identification Media, Chapter 3.)

(2) **Standard** — Managers are responsible for ensuring that only authorized employees are issued pocket commissions and that pocket commissions will only be displayed as prescribed in IRM 1.16.4, Identification Media Handbook. Managers will identify employees who are required to present proof of authority during taxpayer contacts and will initiate requests for pocket commissions for authorized employees. If a category of employees is not on the authorized list, managers will submit a memorandum to their Chief Officer, Operating Division Commissioner, Chief, Criminal Investigation, requesting that the title and series be added to the list. In addition to the title and series, the memorandum will include a justification. Once this request is approved, it should be forwarded to the National Director, Real Estate and Facilities Management Division.

1.16.2.7.7 (03-12-2001)
Pseudonyms

(1) In accordance with the Federal Service Impasses Panel decision dated March 10, 1992, Internal Revenue Service employees authorized to hold a pocket commission may have the pocket commission issued in an approved pseudonym name. In a memorandum dated May 19, 1999, signed by the Chief Operations Officer and the President of NTEU, the Service agreed to issue ID cards in an employee's approved pseudonym name. The pseudonym has to be approved by the employee's manager and a written request from the manager will be submitted to the local Security office asking for issuance of the pocket commission and/or ID card in the employee's pseudonym name.

(2) **Standard** — Employee's may be issued a single ID card and/or pocket commission in an approved pseudonym name. In addition, employees authorized name tags may have the name tag issued in an approved pseudonym name. Managers are responsible for generating requests for issuance of ID media in a pseudonym name. If an employee already has a pocket commission and/or ID card issued in their legal name, that ID media must be recovered prior to issuance of identification media in the pseudonym name. Managers must make sure that employees do not have more then one ID card and/or pocket commission in their possession.

1.16.2.7.8 (03-12-2001)
Calling Cards

(1) Calling cards may be used by Service personnel who have a continuing need to leave their name, unique identifying number and telephone number with non-Service individuals or companies as a ready reference for contact by telephone or at an office address (see IRM 1.16.4, Identification Media Handbook and 1.17, Multi-Media Production).

a. The Form 4811, a blank contact form that allows employees to fill in name (or pseudonym), unique identifying number and telephone number, is available to authorized employees upon approval by

Operating Division Commissioners, Chief Officers, Chief of Criminal Investigations, Regional Commissioners, District Directors and Chief Counsel or their designated officials. The forms may be ordered through the Service's distribution centers by authorized points of contact.

b. The Service recognizes that some individuals may have a need for a personalized calling card. Although there are some exceptions, generally personalized calling cards will be obtained at the employee's personal expense.
c. In order to facilitate compliance with the new statutory requirement of section 3705(a) of the Restructuring and Reform Act of 1998, Treasury has granted an exception to their general policy of not providing personalized business cards at Government expense. The Service will provide ***"eligible employees"*** (that is employees with significant public contact), at no cost to the employee, business cards with the employee's name (or pseudonym name) and unique identifying number.

(2) **Standard**—

a. Personalized business cards, obtained at an employee's personal expense, shall conform to a standard design for uniformity and quality control and must conform to the standards specified by the Service. All requests must be approved by an authorized official or his/her designated representative.
b. Employees having significant public contact may request personalized business cards funded by the Service. The request will certify that the employee regularly deals with taxpayers or organizations concerning official tax matters pursuant to Section 3705(a) of the Restructuring and Reform Act of 1998, will be certified by an authorized management official, will be approved by management and will conform to all guidelines and requirements of the Department of Treasury. Employees providing inaccurate or false information in applying for service funded business cards are subject to appropriate disciplinary action, up to and including removal from Federal service.
c. Management will make sure that employees use business cards for official business only and do not independently generate business cards associating them with the Service. Business cards are considered ID media and must be approved by the Service and comply with Service standards.

1.16.2.7.9 (03-12-2001)

Employee Name Tags

(1) Employees assigned to walk-in areas may be provided name tags as an alternate form of identification in order to meet requirements of 3705(a) of the Restructuring and Reform Act of 1998.

(2) **Standard** — Employee names tags will be issued only to those individuals assigned to taxpayer walk-in areas and will include the employee's name (or pseudonym name) and unique identifying number. The design and size of the name tag will meet Service standards and will be ordered through the employee's manager.

1.16.2.8 (03-12-2001)
Reviews

(1) The Service has established minimum security standards and requirements for which Service managers are responsible. Periodic assessments and reviews assist security personnel and management officials in determining the effectiveness and appropriateness of existing safeguards and security guidelines.

1.16.2.8.1 (03-12-2001)
Assessments

(1) Security measures should relate to the type of risks to which a facility and its contents are exposed, the probability that these risks will occur, and the impact that an occurrence would have on the organization. The risk assessment is used to develop a tailored protective system for the facility and associated annexes. The process should provide an objective tool to identify and justify security measures needed to protect IRS assets and systems.

(2) **Standard** — A risk assessment should be conducted prior to relocating to a new site, if the demographics surrounding the site have changed or if significant incidents have occurred at or around the facility, or at least once every five years. Management may delay the assessment beyond the five year requirement if they can verify that the surrounding area has had no significant change in demographics, no significant incidents or threats have occurred and the mission of the facility has not significantly changed since the last assessment. The risk assessment process is contained in the Consolidated Physical Security Standards for IRS Facilities.

1.16.2.8.2 (03-12-2001)
Functional Reviews

(1) Functional reviews measure adherence to security requirements and procedures that apply to each manager's office or functional area. Functional reviews allow managers to ensure that existing security procedures and requirements are being followed on a daily basis.

(2) **Standard** — First line managers will conduct functional reviews on at least an annual basis or more frequently, will document the review and will provide a copy of the report to the local Security office for review. Managers will maintain a copy of the report for at least 3 years. Review criteria may be based on local concerns but at a minimum managers will conduct an after hours review and will evaluate their areas on:

- Clean Desk Policy
- Disposition of Waste Material
- Locks and Keys
- ID Media
- Security Awareness
- Protection of Sensitive Information

1.16.2.8.3 (03-12-2001)
After Hours Review

(1) An after hours review allows managers to determine whether documents, property and monies are being adequately protected when not in the custody of authorized IRS personnel.

(2) **Standard** — Managers should periodically review functional areas after hours to determine if sensitive information is appropriately containerized and disposed of, whether cabinets, safes and other containers are appropriately secured and whether restricted areas, secure areas and office doors are secured. If weaknesses are identified, managers should take immediate action to safeguard information, property or rooms/facility, counsel employees as appropriate, and/or request assistance from appropriate Security personnel in developing corrective measures.

1.16.2.8.4 (03-12-2001)
Safeguard Reviews

(1) Contracts for services or property which involve the disclosure of sensitive information to a contractor (i.e. return or return information, personnel information and administrative or internal management information critical to mission of the Service), must include appropriate protective measures in accordance with applicable laws, regulations and procedures.

(2) **Standard** — Managers should make sure that requests for contracted services involving disclosure of tax data or other protected information are reviewed by Disclosure and, where appropriate, Security and include:

- a narrative statement of work describing all intended requirements and applications,
- a statement identifying the data to be disclosed,
- proposed security safeguards to protect the data which must be disclosed to the vendor/contractor, or a statement that additional safeguards are not a requirement,
- a statement that a pre-award site survey is or is not required.

1.16.2.8.5 (03-12-2001)
Site Survey

(1) In order to ensure that a contractor facility provides required security safeguards, an on-site (safeguard) review may be required. If it has been determined that a site survey will be required, the contracting officer shall require the vendor to provide, in writing, as part of their offer the following information:

- A copy of internal security review and findings conducted within the previous 12 months,
- A narrative description of the vendors proposal to comply with required safeguards,
- A copy of all of the vendor's policies and procedures relating to security,
- An organization listing or chart, if available.

(If the contract is for automated information services see IRM 2.1.10, Information Systems Security Handbook.)

(2) **Standard** — It is the responsibility of the requesting activity to ensure that a site survey is conducted when necessary. If technical expertise is not available on the user's staff, assistance from Security personnel should be requested. The site review will usually consist of a pre-review conference, interviews, facility tour and close out conference.

a. Pre-review conference should be held with reviewer, Security personnel, as appropriate and the contractor to determine the scope and methodology of the review.
b. Interviews with contractor employees should be held to ascertain the level of security maintained and degrees of security awareness. The interview scheduled should be arranged during the pre-review conference.
c. A tour of the contractor's facility should be conducted and should follow the flow of IRS data from point of receipt to point of final disposition.
d. A close-out conference allows the reviewer to clarify any areas of concern and provides an opportunity to discuss deficiencies or vulnerabilities.

1.16.2.8.6 (03-12-2001)

Recertification

(1) An existing contractor's ability to adequately protect IRS data from unauthorized use or disclosure must be recertified annually for contracts which extend beyond a one year period, prior to contract renewal or if the safeguards employed by the contractor become a matter of concern (e.g. suspected security breach).

(2) **Standard** — The requesting function is responsible for contract recertifications. If the recertification is conducted due to a disclosure concern, Security personnel should be contacted and briefed on the areas of concern. The contractor will be requested to provide a self-assessment regarding their ability to protect IRS data. If it cannot be determined from the self-assessment and other documentation whether to recertify, a recertification site review of the contractor facility should be scheduled.

This page intentionally left blank.

Exhibit 1.16.2-1 (03-12-2001)
Protection Alternative Chart
Alternative Chart

Protected Item Classification	IRS Perimeter Type	Interior Area Type	Container Type
Normal Security			
Alternative #1	Locked		
Alternative #2		Locked	
Alternative #3			Locked
High Security			
Alternative #1	Secured		Locked
Alternative #2	Locked	Secured	
Alternative #3	Locked		Security
Special Security			
SP-1	Locked		Safe/Vault
SP-2	Locked		Security
SP-3	Locked		Locked

* Sp-2 and High Security, Alternative #3 appear to be the same. The difference is that SP-2 items ***"must"*** be stored in a locked container, whereas High Security items may be stored in a Security container, a secured room or in a locked container within a secured IRS perimeter.

Exhibit 1.16.2-2 (03-12-2001)
Protectable Items

Designation	Item
SP-3*	Adverse Action and Adverse Action Appeal Files
NS**	All material, not classified as requiring high security or special protection.
HS***	All portable equipment which can be stored in a standard pull drawer or lateral file cabinet. This includes laptop computers, combination padlocks, cameras and similar highly portable items. ***(Note:*** Laptops can be secured using commercially available hardware designed to secure computers when not stored as required above.)
SP-3	Annual Listing of Undelivered Refund Checks
SP-2****	Ammunition
HS	Assault and Threat Reports
SP-3	Bills of Lading — Blank GBL's
SP-2	Checks Drawn on U.S. Treasury (except those endorsed to the IRS for the payment of taxes).
SP-3	Checks Received for Payment — including personal checks, cashiers checks, bank draft, money orders and U.S. Treasury checks endorsed to the IRS for the payment of taxes. ***(Note:*** In service center must be in secured area or containerized.)
HS	Classification Stamps — "accepted as filed"
	Classified Information — Top Secret/Secret/Confidential (see 1.16.31)
SP-2	Combination Records (Forms 700 for container or doors)
SP-1	Combination Records (Forms 700 for safe and vaults)
HS	Coordinated Examination Records — including all open or closed project files, case files, correspondence, activity reports, and other material which contains taxpayer data or third party information acquired in connection with a planned, open or closed case
SP-1	Currency over $1,000
SP-2	Currency up to and including $1,000
NS	Currency Transaction Reports — Forms 4789
SP-2	Director's Seal
HS	Disclosure Records relative to disclosures made to Department of Justice, Executive Departments, or Congressional Committees
HS	Discriminant Function (DIF) formulas, program requirements packages and related materials
SP-3	Employee Underreporter Program/Cases

Exhibit 1.16.2-2 (Cont. 1) (03-12-2001)
Protectable Items

Designation	Item
HS	Examination Records — those maintained at the request of Congressional Committees
HS	Examination Selection, Criteria and Formulas, Cycle Variables and Volume Controls
SP-1	Firearms (over 4)
SP-2	Firearms (up to and including 4)
SP-2	Four (IV) Phase Operator's Listing
SP-2	Four (IV) Phase C-Type Audit Trial Listing
SP-2	Four (IV) Phase Master List of System Users
SP-2	Four (IV) Phase Job Directory Listing
SP-2	Four (IV) Phase Change Requests (Form 6610)
SP-2	Four (IV) Phase Password List
HS	Fraud Referrals — all case files, correspondence, or related documents which contain information regarding items referred to Criminal Investigation
HS	General Ledger and Subsidiary Records — revenue accounting only
SP-3	All Government issued credit cards
SP-2****	Grand Jury — Case file and information
SP-3	Grievance Files and Grievance Appeal Files
SP-2	IDRS Passwords and Password Registers
SP-3	IDRS Security Handbook
SP-2	IDRS Security Records (including PRP's, reports, control documents, audit trail records and computer tapes)
SP-2	Identification Media (IRS) — all unused stock and completed media which is not in the possession of the employee to who it is assigned
SP-3	Identification Media (IRS) — completed non-photo visitor and temporary cards
SP-2	Informant Communications File
SP-2	Informants' Claims for Reward
SP-2	Informants' Control File
SP-3	Internal Security Records — including all open or closed investigate reports, informant files, and other material that contain investigative information concerning employees and/or taxpayers, or taxpayer data, third party information, tax data, or specific information concerning Service operations acquired in connection with a planned, open or closed case.

Exhibit 1.16.2-2 (Cont. 2) (03-12-2001)
Protectable Items

Designation	Item
SP-3	Internal Audit Records — including Internal Audit Reports and workpapers, open or closed, and other material containing tax data, taxpayer information, functional records and information concerning service center operations, acquired in connection with planned, open or closed audits.
SP-3	Internal Revenue Service Employee — delinquency
NS	Investigative Equipment — equipment specifically acquired and used by Criminal Investigation and Internal Security for carrying out investigation and enforcement functions.
SP-3	Key — to any locked container
SP-2	Key — to any room, area, secured area, or security container
SP-3	Law Enforcement Manual (LEM) (Normal Security will apply to service centers)
HS	Legal Case Files and Records of Chief Counsel, Deputies Chief Counsel, and their Assistants
SP-2	LIMITED OFFICIAL USE documents
HS	Magnetic Media — all discs, tapes or similar media which contain program, taxpayer or other individual data
SP-3	Medical Records — employee health records, disability retirement records, and similar files containing personal medical information
HS	Microfilm — all cartridges, cassettes or other microfilm media which contain taxpayer data or account information.
SP-3	Minority Group Designator Data
SP-2	Negotiable and Non-negotiable Instruments — including stocks, bonds, securities or other collateral
SP-3	OFFICIAL USE ONLY Documents (unless otherwise increased by the originator)
SP-3	Personnel Records — including personnel folders, investigation reports, qualification statements, and other records containing privacy act or sensitive information
HS	PRP 160, Section 26 (SERFE)
SP-2	Receipts — unissued Forms 809 (CP-444) or 4733 (CP-445)
NS	Received Stamps
HS	Received with Remittance Stamps
SP-2	Relocated Witness Files
HS	Risk Analysis Final Reports and associated supporting documentation
HS	Sensitive investigative equipment — devices that can be used in the interception of telephonic communications or non-telephonic communications

Exhibit 1.16.2-2 (Cont. 3) (03-12-2001)
Protectable Items

Designation	Item
HS	Signature Stamps or Facsimile Signature Plates
HS	Statutory Notices — signature stamps or facsimile signature plates
SP-3	Form 6888, US. Government Purchase Order — invoice voucher (unissued stock)
HS	Taxpayer and Privacy Act Information (due to the protection provided, service and computing centers are exempt from this requirement)
HS	Tax Practitioner File — including extension files
HS	TECS Data — which contains information regarding the involvement of Criminal Investigation with taxpayers of third parties
SP-3	Test Materials — OPM, IRS and commercial
HS	Testimony of IRS Employees in Non-tax matters
SP-3	Training Records — including individual ratings, examination record and register cards, and similar individual test result information
SP-3	Transportation Requests — blank and unissued TR's
HS	Unapplied Master File Credit Records
SP-3	Undelivered Refund Check Notices
SP-3	Unidentified Remittance Record
HS	Unit Ledger Cards
*SP	SPECIAL SECURITY
**NS	NORMAL SECURITY
***HS	HIGH SECURITY
****	If volume dictates, these items may be stored in a security room as specified in Chapter 4 of this Handbook